Department of Homeland Security Daily Open Source Infrastructure Report for 20 June 2006

Current Nationwide Threat Level is ELEVATED Significant Risk of Terrorist Attacks
For info click here
http://www.dhs.gov/

Daily Highlights

- MarketWatch reports the Social Security numbers and other personal information for 13,000 District of Columbia workers and retirees are now in the hands of thieves who stole a laptop from the home of an ING U.S. Financial Services employee last week. (See item 18)
- The New York Times reports federal investigators are concerned about an engine break−up that nearly destroyed a Boeing 767 on the ground in Los Angeles, because the failure may indicate a recurrence of a problem they thought they had eliminated in 2003. (See item 21)
- The Saginaw News reports railroad officials have said the derailment of a train carrying radioactive material from Michigan's defunct Big Rock Nuclear Power Plant appears an act of sabotage. (See item 24)

Energy Sector

Current Electricity Sector Threat Alert Levels: Physical: ELEVATED, Cyber: ELEVATED
Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES−ISAC) − http://www.esisac.com]

1. *June 19, Associated Press* — **Ford prepares to roll out fumes−to−fuel system at plants.** Ford Motor Co. is preparing to roll out a system to capture toxic paint fumes and convert them into electrical power. Priming, painting, and clear coating millions of new cars and trucks every year creates millions of pounds of waste at plants around the world. Currently, paint fumes at auto

plants are collected and burned in incinerators. Paint overspray is captured, treated, and consolidated into nonhazardous sludge that is eventually dumped in landfills. Ford first tested the fumes−to−fuel system in 2004. Two years later, Ford is wrapping up a pilot program at the Michigan Truck Plant and preparing to roll out the system at other plants as equipment is updated and replaced.
Source: http://thestaronline.com/news/story.asp?file=/2006/6/19/apworld/20060619080005&sec=apworld

2. *June 18, Associated Press* — **U.S. lawmakers push sugar as fuel source.** With the market for corn−based ethanol booming, lawmakers from sugar−producing U.S. states are hoping that beet and cane growers can soon jump onto the renewable fuel bandwagon. They cite the model of Brazil, which produces ethanol made from sugar cane. Critics question whether the economics of sugar−based ethanol would work in America. The U.S. Department of Agriculture is expected to issue a long−awaited study around July 1 on the viability of converting sugar into ethanol.
Source: http://www.thestate.com/mld/thestate/news/nation/14849103.ht m

3. *June 17, Associated Press* — **Union Pacific sets a record for coal.** Strong demand for coal and agriculture products helped boost shipping volume for Union Pacific Corp. five percent in the second quarter through June 10, the railroad said Friday, June 16. Union Pacific's intermodal shipping, which uses large containers that can be carried by railroads, trucks, cargo planes, or ships, has set company volume records every month in 2006. The railroad said energy shipping is up about eight percent in the quarter, and May was a record month for coal shipped from Wyoming's Southern Powder River Basin. Union Pacific is also transporting more ethanol shipments this year than it did last year.
Source: http://www.chron.com/disp/story.mpl/business/energy/3977964. html

4. *June 15, Utility Automation & Engineering* — **Consumers making few energy related lifestyle changes: study.** A new survey conducted by the Energy & Resources industry practice of Deloitte & Touche USA LLP finds that, in spite of high energy prices, only one−third of consumers have made lifestyle changes to lower electricity consumption. While consumers have significant concerns about natural gas prices and some concern about electricity prices, they are most concerned about the cost of gasoline. Eighty−nine percent are very concerned about current gasoline prices, which have risen 27 percent between May 2005 and May 2006. However, the study found that nearly two−thirds of consumers have not made lifestyle changes to decrease electricity use. Of those who did alter their behavior, the most common action was to adjust the thermostat, with only 20 percent conducting any actual energy efficiency improvements or purchasing energy efficient appliances. Regarding nuclear power, the study found that, compared to past studies, there is a higher level of support, with nearly half in favor.
Source: http://uaelp.pennnet.com/Articles/Article_Display.cfm?ARTICL E_ID=257798&p=22

[Return to top]

Chemical Industry and Hazardous Materials Sector

5. *June 19, Associated Press* — **Chemical plant in Michigan releases gas.** A Muskegon County,

MI, chemical plant has been shut down as authorities investigate the Friday, June 16, release of nitric oxide gas. About 200 area residents were forced indoors and some businesses were closed for a few hours.
Source: http://www.9and10news.com/News/Story.asp?StoryID=51966

6. *June 19, Tampa Bay's 10 News (FL)* — **Diesel spill prompts road closure in Florida.** Workers started cleaning up diesel−contaminated dirt Monday, June 19, in Tampa, FL, after a gasoline tanker overturned Sunday, June 18, spilling 200 gallons of fuel. Cross Creek Boulevard and Morris Bridge Road were both shut down for more than eight hours Sunday because of the incident.
Source: http://www.tampabays10.com/news/local/article.aspx?storyid=3 3687

7. *June 19, NBC5i (TX)* — **Chemical fumes force hotel evacuation in Texas.** An Arlington, TX, hotel was evacuated overnight Sunday, June 18, after several residents became sick. Firefighters evacuated the Admiral Hotel after chlorine fumes made several people ill. The cause: Chlorine tablets, intended for the pool, got wet after being left in a hallway.
Source: http://www.nbc5i.com/news/9390248/detail.html

8. *June 19, Houston Chronicle* — **Shelter−in−place ordered after Shell leak.** The floating roof of a chemical storage tank at Shell's Deer Park, TX, chemical plant tipped open under the weight of pooling rain water Monday morning, June 19, exposing chemicals, including benzene, to the atmosphere. The release of vapors from the tank led officials to call for a shelter−in−place for areas north of San Augustine Street between Center Street and Georgia. Highway 225 from Battle Ground Road to Beltway 8 was also closed.
Source: http://www.chron.com/disp/story.mpl/business/energy/3982897. html

9. *June 19, Associated Press* — **Railroad investigating chemical spill that snarled commuting.** The Burlington Northern−Santa Fe Railway Company is still investigating what caused one of its trains to spill several bags of acid powder along the tracks west of Chicago last week. As many as 35 bags of stearic acid had been scattered along a 27−mile stretch between Cicero and Aurora. The spill stranded thousands of Metra commuters train riders for as long as four hours Thursday evening, June 15. Delays and cancellations continued Friday morning, June 16.
Source: http://abclocal.go.com/wls/story?section=local&id=4284212

[Return to top]

Defense Industrial Base Sector

10. *June 19, Government Accountability Office* — **GAO−06−739R: Defense Management: Attention Is Needed to Improve Oversight of DLA Prime Vendor Program (Correspondence).** In 1992, the Government Accountability Office (GAO) identified the Department of Defense's (DoD) contract management as one of their high−risk areas, and it remains so today. One of the key reasons the area is high risk is because DoD does not provide adequate oversight over defense contracts. One aspect of oversight is to ensure that the government is obtaining fair and reasonable contract prices through such means as conducting price reviews. In addition, management oversight can also assure that steps are taken to

determine that prices agreed to at contract award are fair and reasonable. For the purposes of this report, GAO defines a pricing review as either a determination of price reasonableness for items added after the initial contract award, or a post−award verification that any invoiced price is not in excess of the price stipulated in the contract. Under the authority of the Comptroller General, GAO initiated a review of DoD's prime vendor concept to determine (1) the extent to which the Defense Logistics Agency (DLA) has conducted pricing reviews for items purchased through a prime vendor, and (2) the extent to which DLA has addressed the pricing issues identified at the November 2005 hearing.
Source: http://www.gao.gov/cgi−bin/getrpt?GAO−06−739R

11. *June 16, RAND Corporation* — **A brief analysis of the Republic of Korea's Defense Reform Plan.** At the request of Republic of Korea (ROK) Assemblyman Jin−Ha Hwang, a member of the National Assembly's National Defense Committee, the RAND Corp. was asked to perform analysis of the ROK Defense Reform Plan (DRP). It examines the overall nature of the DRP, identifies major risks in the plan, and discusses how those risks can be managed. It concludes that the DRP is a good approach to potential ROK security dilemmas, but the plan faces major risks, especially in meeting potential ROK security requirements. The DRP could be strengthened by adding concepts for managing its major risks.
The full report: http://www.rand.org/pubs/occasional_papers/2006/RAND_OP165.p df
Source: http://www.rand.org/pubs/occasional_papers/OP165/

12. *June 16, CongressDaily* — **Bush signs supplemental spending bill.** President Bush Thursday, June 15, signed a $94.5 billion fiscal 2006 supplemental appropriations bill that funds military operations in Iraq and Afghanistan, hurricane relief efforts and avian flu preparedness, after the Senate earlier in the day approved it 98−1. The underlying bill also sets an $873 billion fiscal 2007 discretionary spending cap, a 3.6 percent increase over this year's spending, so the Senate can move ahead with appropriations bills.
Source: http://www.govexec.com/story_page.cfm?articleid=34344&dcn=to daysnews

13. *June 15, Federal Times* — **U.S. defense officials seek private help for overseas military mail delivery.** U.S. defense officials have put out a call to the private sector for ideas on how they could deliver overseas military mail more efficiently. Officials issued a request for information Wednesday, June 14, asking for "unique and innovative ideas or approaches that have been developed outside of the government... that encompass a comprehensive review of the Military Postal System." This request will not result in a contract. However, depending on the information received, the government could issue a request for proposals that could result in a contract to outsource military mail.
Source: http://federaltimes.com/index.php?S=1875562

[Return to top]

Banking and Finance Sector

14. *June 19, Channel Register (UK)* — **Customers caught in National Australia Bank phishing attack.** A phishing email claiming that The National Australia Bank (NAB) is bankrupt has caught more than 1,000 of the bank's customers. The e−mail warns the bank's customers that

NAB might be bankrupt. It claims the bank's ATMs are not working and that people are starting panic withdrawals. It invites them to click on a link that will provide them with more information. The e−mail downloads a Trojan onto the banker's machine, which steals their bank login details and password when they follow the rest of the e−mailed "advice" to go online to check their balance. The code exploits a well−known flaw in IE to do its dirty work, and is a variation of the Banker virus, discovered by Websense in early April. Microsoft issued its patch shortly afterwards. Firefox users might also be vulnerable, according to reports.
Source: http://www.channelregister.co.uk/2006/06/19/bank_details_aus sies/

15. *June 19, Computeractive* — **PayPal fixes phishing flaw.** Paypal has blocked a sophisticated attack that tricked users of the online payment service into visiting a phishing site. The flaw in the PayPal Website allowed cyber−criminals to host a page on PayPal's Website. The Web pages appeared with a genuine SSL certificate to lull users into a false sense of security. Malicious code on the fake page warned people that their PayPal account had been compromised. People were then redirected away from the genuine PayPal site to a phishing site hosted in South Korea. Here victims were asked for their PayPal login information. According to Internet monitoring company Netcraft, which first raised the alarm about the attack on Friday, June 16, people were also asked to enter their Social Security number and credit card details. PayPal said it changed some code on the PayPal Website to block the scam.
Source: http://www.computeractive.co.uk/computeractive/news/2158530/paypal−fixes−phishing−flaw

16. *June 19, Computer Crime Research Center* — **FBI opens new cybercrimes unit.** On Tuesday, June 13, the FBI announced the creation of the Metro East Cyber Crimes and Analysis Task Force (MCCA) to assist local police agencies in their investigations. Participating Illinois police departments include Glen Carbon, Southern Illinois University Edwardsville, and the Madison County Sheriff's Department. Janice Fields of the FBI said the FBI and local police are "going to be working as a cohesive group to identify and neutralize one of the most significant threats we have −− cybercrime." She added: "This is a huge agenda for the FBI. Without the assistance from our local law enforcement, we could not do it." In the Metro East, 15 local, state, and federal agencies will share information and resources. The MCCA will be the FBI's 94th cybercrimes task force nationwide.
Source: http://www.crime−research.org/news/19.06.2006/2060/

17. *June 19, VNUNet* — **ID thieves purport Coke lottery win.** Security experts have published details of a newly discovered e−mail−based fraud that tries to ensnare recipients with a bogus notification purporting to be a lottery win from Coca−Cola. The e−mails, which have the subject line 'Coca Cola Promotion', have been spammed out to Internet users claiming that the recipient has won $2.5m in a lottery held by the soft drinks firm earlier this month. The recipient is told that they are one of 50 lucky winners around the world selected randomly after computers found their e−mail address on Internet Websites. To collect their winnings, people are told to call, phone, or fax an agent who claims to be working on behalf of Coca−Cola. However, security firm Sophos warned that the spam is a ruse to steal personal details, and that the scammers can use the information to steal money from bank accounts and commit identity fraud.
Source: http://www.itweek.co.uk/vnunet/news/2158563/id−thieves−brew− coke−spam−scam

18. *June 18, MarketWatch* — **Confidential data at risk after laptop stolen.** The Social Security numbers and other personal information for 13,000 District of Columbia workers and retirees are now in the hands of thieves who reportedly stole a laptop from the home of an ING U.S. Financial Services employee last week, the company confirmed. ING U.S. Financial services manages the District's retirement plan, and notified the city on Friday, June 16, of the laptop theft. The laptop was stolen from the home of an ING financial adviser and agent responsible for overseeing the District's retirement plan. The theft was reported last Monday, but ING took the ensuing days to ascertain what information was stored on the laptop, ING spokesperson Caroline Campbell said. The company is mailing letters to those whose personal data was stored on the computer, and will pay for a year of credit monitoring and identity−theft protection. The data on the laptop is unencrypted. It's unclear whether the thief knows the nature of the data stored on the laptop. Other household items were also reported stolen during the theft. In December, thieves stole an ING laptop that was password−protected, but contained unencrypted data on 8,500 Florida hospital workers.
Source: http://www.marketwatch.com/News/Story/Story.aspx?guid=%7B5EB7D976−2922−4E99−9F6E−B1F323A884FA%7D&print=true&dist=printTo p

19. *June 16, CNET News* — **Data−thieving worm targets Orkut users.** A new worm that attempts to steal online banking credentials is propagating on Google's social−networking Website, FaceTime Security Labs warned Friday, June 16. The worm, dubbed MW.Orc, primarily targets Brazilian users of Google's Orkut Website. It uses a message in Portuguese to entice people to click on a file that is disguised as a JPEG image. The initial file, called "minhasfotos.exe," creates two additional files on a user's system, "winlogon_.jpg" and "wzip32.exe." When the user, after the initial compromise, clicks on the "My Computer" icon in Windows XP, an e−mail with his or her personal data is sent to the anonymous attacker, the security company said. Additionally, the compromised computer may be added to a network of hijacked PCs, known as a botnet. The pest also tries to propagate by placing a malicious link on the profiles of people in the Orkut user's network, FaceTime said. The Orkut worm is targeting Brazilian users in an attempt to steal credentials for Brazilian banks, it is believed.
Source: http://news.com.com/Data−thieving+worm+targets+Orkut+users/2100−7349_3−6084932.html?tag=cd.top

20. *June 16, Computerworld* — **PNC bank warns customers of fraudulent e−mails.** PNC Bank in Pittsburgh, PA, is warning customers not to fall for phishing e−mails purporting to come from the bank. "The e−mail subject titles are: 'Your account has been limited,' or 'Log on Now.' These e−mails were not sent from PNC," the bank said in an e−mail to users Thursday, June 15.
Source: http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9001245&taxonomyId=17

[Return to top]

Transportation and Border Security Sector

21. *June 19, New York Times* — **Airliner engine breaks apart, defying federal repair effort.** Federal investigators say they are deeply concerned about an engine break−up that nearly destroyed a Boeing 767 on the ground in Los Angeles on June 2, because the failure may indicate a recurrence of a problem they thought they had eliminated in 2003. American Airlines

mechanics were testing the engine after the crew of an earlier flight had reported it was not performing properly. During the test, an internal disk came apart, slicing open a fuel tank in the left wing; the fuel spilled onto the ground, where it caught fire. One piece of metal was thrown more than half a mile from the plane. The first such engine explosion occurred in July 1989, during a flight of a United Airlines DC−10. That engine was mounted in the tail, and the debris disabled the plane's hydraulic system; 111 people were killed. In addition, an Air New Zealand 767 suffered an uncontained failure at 11,000 feet on a flight from Auckland, New Zealand, to Brisbane, Australia, in December 2002. That plane landed safely. But as a result, in March 2003, the Federal Aviation Administration ordered inspections of the part involved. The engine in all reported cases was a variation of the popular General Electric CF6.
Source: http://www.nytimes.com/2006/06/19/washington/19plane.html?_r =1&oref=slogin

22. *June 19, Associated Press* — **Mayor Bloomberg suggests return of seaplanes to ease airport congestion.** More than 60 years after the Pan American flying boat Yankee Clipper departed Long Island Sound on its last trans−Atlantic flight, New York City's mayor says it may be time to resurrect the seaplane to ease pressure on the city's crowded airports. During a recent radio talk show, Mayor Michael Bloomberg noted that airport and ground facilities lag behind the growth of intercontinental jet travel. "If you take a look at a map, one thing we have going for us is an enormous runway all around −− it's called the water," he said. "For local, short flights, to let's say, Boston, Chicago, Atlanta, Florida ... you can land out away from everybody and then taxi in." Most seaplanes today are small aircraft built in Canada, Japan, and the United States. They're used for short commuter flights and island−hopping sightseers. Only Russia builds what Bloomberg called "enormous seaplanes" that carry 50 or 100 people. LaGuardia Airport's Marine Air Terminal, the New York base for the Pan Am flying boats, fell into neglect after their demise. Since refurbished as an art−deco landmark, it still serves corporate aircraft and Delta Airlines' shuttle to Chicago.
Source: http://www.usatoday.com/travel/news/2006−06−19−seaplanes_x.h tm

23. *June 19, USA TODAY* — **Small airports get screeners as big terminals suffer.** Last year, passengers at Kahului Airport in Maui, Hawaii, breezed through some of the fastest security lines in the nation. On the other end of the country, Orlando, FL, travelers stood in lines that exceeded federal waiting−time goals every day. Even so, in July 2005, the Transportation Security Administration (TSA) increased the number of security screeners at smooth−running Kahului by 26 percent. And in crowded Orlando, it cut the screener workforce by 10 percent. According to a USA TODAY analysis of data from 80 major airports, the experiences of Kahului and Orlando illustrate the confounding way the TSA allocates one of the most precious airport resources, security screeners, and the agency's inability to create consistent wait times in security lines across the country. In Orlando, with about 94,000 passengers a day, security lines ran 30 minutes or more 241 times in the first four months of the year. That prompted the airport to spend $1.8 million in April to hire a company to help passengers move through checkpoints faster. TSA is adopting a more flexible system that gives local airport security directors greater control over staffing and evaluates the efficiency of an airport's security lines to determine whether it needs more screeners.
Source: http://www.usatoday.com/travel/news/2006−06−18−airport−waits_x.htm

24. *June 19, Saginaw News (MI)* — **Train derailment called sabotage.** The derailment of a train carrying radioactive material from the defunct Big Rock Nuclear Power Plant, near Charlevoix,

MI, appears an act of sabotage, railroad officials said on Monday, June 19. "We feel strongly there was some tampering, some vandalism going on," said Mike Bagwell, chief executive of Tuscola and Saginaw Bay Railway. Seventeen of the train's 38 cars left the tracks on Friday, June 16, as it traveled through a switch near the Renosol Corp. plant in Surrey Township, MI, Clare County officials have said. Authorities have no specific suspects, but the cars jumped the line midway through the switch. Two locomotives and four cars traveled safely through the line change when the switch suddenly diverted the train, Bagwell said. The switch operates manually, but Bagwell said it was not likely that someone was present to make it occur. A green light tricked the engineer into thinking the switch was safe, he said. Bagwell also said that despite the sabotage, he did not believe the train was targeted because of the radioactive shipment. No one was injured in the wreck.
Source: http://www.mlive.com/news/sanews/index.ssf?/base/news−3/1150723335185740.xml&coll=9

[Return to top]

Postal and Shipping Sector

Nothing to report.
[Return to top]

Agriculture Sector

25. *June 19, Illinois Ag Connection* — **State livestock health papers go electronic.** Illinois livestock producers and veterinarians may use electronic health certificates to help with interstate movement of animals, according to Mark Ernst, Illinois state veterinarian. The Illinois Department of Agriculture (IDOA) works an Internet−based service for accredited veterinarians, to provide electronic certificates for Illinois, Ernst said. An accredited veterinarian obtains a password from the Web service, and then logs onto the site. The veterinarian completes the health certificate online and then may forward a copy to the state of destination, Ernst said.
Source: http://www.illinoisagconnection.com/story−state.cfm?Id=533&y r=2006

26. *June 15, Black Hills Pioneer (South Dakota)* — **Four elk test positive for chronic wasting disease.** Thirteen elk and eight deer were tested for chronic wasting disease (CWD) over the winter at Wind Cave National Park, in South Dakota, with the results just now becoming available. Animals tested came from road−killed animals and targeted surveillance for elk demonstrating clinical signs of the disease. Since 1998, 123 deer and 34 elk in Wind Cave National Park have been tested for CWD. Of those animals, eight deer and eight elk have tested positive for the disease.
CWD information: http://www.cwd−info.org/
Source: http://www.zwire.com/site/news.cfm?newsid=16795791&BRD=1300&PAG=461&dept_id=156923&rfi=6

[Return to top]

Food Sector

27. *June 19, Cattle Network News* — **Japan to decide on U.S. beef imports.** Japan plans to decide the week of Sunday, June 18, on when to remove a ban on U.S. beef imports imposed over fears of made cow disease. "We want to show a sense of direction next week. By taking into account the various opinions that have been exchanged, we are going to take the next step," Agriculture Minister Shoichi Nakagawa told reporters Friday, June 16. He said his ministry will develop measures to ensure safety, such as a potential dispatch of Japanese inspectors to U.S. meatpackers.
Source: http://www.cattlenetwork.com/content.asp?contentid=45719

28. *June 19, Associated Press* — **Five workers from a beef plant arrested.** Five workers from National Beef's plant in Liberal, KS, have been indicted on federal immigration charges, the U.S. attorney's office announced Thursday, June 15. All five had worked at the plant at least two years and used names and Social Security numbers of U.S. citizens to get the jobs, the U.S. attorney's office said.
Source: http://www.kctv5.com/global/story.asp?s=5036575&ClientType=P rintable

[Return to top]

Water Sector

Nothing to report.
[Return to top]

Public Health Sector

29. *June 19, Xinhua (China)* — **China reports new bird flu outbreak.** A new bird flu outbreak has been reported in north China's Shanxi Province, said sources with the Ministry of Agriculture Monday, June 19. The outbreak was identified after chickens died in poultry farms in Changzi County of Changzhi City. Samples of the dead poultry were sent to the national bird flu laboratory and the H5N1 virus was identified in them, said the ministry. The local government has launched an emergency response and quarantined the infected area. Experts and veterinarians have started disinfection and culling poultry in the area to prevent possible new outbreaks. A human case of bird flu was confirmed on June 15 in south China's Guangdong Province, bringing the country's total human infections to 19.
Source: http://www.chinadaily.com.cn/china/2006−06/19/content_620828 .htm

30. *June 19, Thanhniem (Vietnam)* — **Cat infected by bird flu detected in Indonesia.** A cat infected by the H5N1 strain of bird flu has been detected in Indonesia, said Steven Bjorge, medical officer for the World Health Organization's (WHO) Communicable Disease Section, Monday, June 19. Bjorge, speaking in a panel discussion at the Jakarta Foreign Correspondents' Club, said he thinks the cat "was infected by probably eating contaminated birds." There are no recorded cases of cat−to−human H5N1 infection anywhere in the world. Trisatya Naipospos, the government's top adviser on H5N1 strategy, told the panel there have been unpublished studies of other cats in Indonesia being tested positive for the H5N1 strain of bird flu. There

have been a number of cases of feline infection by the dangerous H5N1 strain of avian flu outside of Indonesia, all of which appear to have been associated with outbreaks in domestic or wild birds and acquired through ingestion of raw meat from an infected bird.
Source: http://www.thanhniennews.com/healthy/?catid=8&newsid=16784

31. *June 02, RAND Corporation* — **Organizing state and local health departments for public health preparedness.** Improving the ability to respond to bioterrorism and other emergencies is an important challenge facing the U.S. public health system. Despite having a knowledgeable workforce, practice and experience, capacity, and partnerships with other responders in the community, the system's ability to respond may depend largely on its structure. The RAND Corp. published a study that examines a key question: Are state and local public health agencies related to one another in a way that facilitates emergency response? Specific objectives of this study were to explain the factors influencing the particular ways in which state and local public health systems are organized, how the various types of relationships that exist between state and local public health departments have been arrived at, and, most important, the consequences of such structures and relationships for emergency preparedness.
The full report: http://www.rand.org/pubs/technical_reports/2006/RAND_TR318.p df
Source: http://www.rand.org/pubs/technical_reports/TR318/

[Return to top]

Government Sector

32. *June 19, Government Accountability Office* — **GAO−06−895T: Immigration Enforcement: Weaknesses Hinder Employment Verification and Worksite Enforcement Efforts (Testimony).** The opportunity for employment is one of the most important magnets attracting illegal immigrants to the United States. The Immigration Reform and Control Act (IRCA) of 1986 established an employment eligibility verification process and a sanctions program for fining employers for noncompliance. Few modifications have been made to the verification process and sanctions program since 1986, and immigration experts state that a more reliable verification process and a strengthened worksite enforcement capacity are needed to help deter illegal immigration. This testimony is based on the Government Accountability Office's (GAO) August 2005 report on the employment verification process and worksite enforcement efforts. In this testimony, GAO provides observations on (1) the current employment verification process and (2) U.S. Immigration and Customs Enforcement's (ICE) priorities and resources for the worksite enforcement program and the challenges it faces in implementing that program. GAO recommended that the Department of Homeland Security (DHS) set time frames for completing its review of the Form I−9 and that U.S. Citizenship and Immigration Services in DHS assess the costs and feasibility of addressing Basic Pilot Program weaknesses. DHS agreed with these recommendations and is taking steps to assess the pilot program's weaknesses.
Highlights: http://www.gao.gov/highlights/d06895thigh.pdf
Source: http://www.gao.gov/cgi−bin/getrpt?GAO−06−895T

[Return to top]

Emergency Services Sector

33. *June 19, Federal Computer Week* — **Roadblocks hamper emergency response system coordination.** Five years following 9/11, emergency preparedness at the federal, state and local levels continues to lurch toward seamless information exchange −− the backbone of coordinated emergency response. Achieving interoperable communications −− a Holy Grail of sorts for first responders −− is easier said than done. That was the consensus of information technology experts who met earlier this month in Washington, DC, for the National Association of State Chief Information Officers' midyear conference. Participants in a panel discussion said progress has been slow and erratic. The discussion was titled "Our Next Emergency Is Here −− Any Progress on Communications Interoperability?" The uncoordinated deployment of emergency communications systems undermines the goal of interoperability, IT experts say. Money pouring into local jurisdictions from the Department of Homeland Security is fueling the problem, they say, by allowing localities to purchase communications systems without regard for common technical standards.
Survey results: http://www.fcw.com/images/st_images/techchart_06_19_06.pdf
Conference Website & on−site survey results:
http://www.nascio.org/events/2006MidyearConference/#ars
Source: http://www.fcw.com/article94886−06−19−06−Print

34. *June 17, Daily News (CA)* — **Ham radio operators to conduct preparedness exercise.** Ham radio operators, who provide critical communication services in emergencies, will show off their skills this weekend in an overnight exercise. The Santa Clarita Amateur Radio Club, W6JW Inc., will hold a live demonstration of emergency communications abilities in Saugus, CA. Using only generators, batteries or solar power, the hams will construct emergency stations in parks, shopping malls and local hilltops to test their emergency and disaster communications skills under all situations. This annual Field Day is the climax of the weeklong Amateur Radio Week sponsored by the national association for amateur radio. More than 30,000 amateur radio operators across the country participated in last year's event.
Source: http://www.dailynews.com/antelopevalley/ci_3947350

35. *June 17, Tucson Citizen (AZ)* — **Lawmaker says Arizona county's homeland security money wasted; auditor faults controls.** The state auditor and a lawmaker from Tucson, AZ, are questioning the supervision and use of federal homeland security funds in Pima County. The grant funds have been spent on computers for Pima County park patrol cars, biohazard suits for Pima Community College police and Neighborhood Watch signs for Tucson, among other things. The purchases show the need for more oversight of homeland security spending in Arizona, according to state Rep. Jonathan Paton (R−AZ). The Neighborhood Watch signs exemplify how the grants are sometimes spent on projects with little or no connection to homeland security, Paton said. Other expenses raise questions of duplication, according to Paton. Pima College police, for instance, used a $10,000 grant to buy biohazard protection. The college doesn't need such equipment when Tucson emergency responders have it and can be sent to the college, Paton said.
Source: http://www.tucsoncitizen.com/daily/local/16242.php

[Return to top]

Information Technology and Telecommunications Sector

36. *June 19, IDG News Service* — **Nokia and Siemens to merge telecom infrastructure units.** Nokia and Siemens announced on Monday, June 19, that they will merge their telecommunications infrastructure units to form Nokia Siemens Networks, the third such combination formed recently and an indication of the growing competitive pressures in the telecom supplier market. Nokia and Siemens said that the new company will be able to compete better with the growing threat from Asian suppliers and offer more innovative converged wireline and wireless products.
Source: http://www.infoworld.com/article/06/06/19/79405_HNnokiasieme ns_1.html

37. *June 19, Newsfactor Magazine Online* — **Exploits circulating for unpatched Windows PCs.** Although Microsoft released a string of patches to fix security flaws in Windows and Microsoft Office last week, security experts are warning of several "in−the−wild" exploits that are now targeting unpatched systems. In recent months, hackers have increased the speed at which they can create malicious software that targets security flaws for which patches have just been issued. Whenever a patch is issued, it typically comes with an extensive advisory that details the vulnerability and the effect the patch might have on other software. This information allows hackers to begin building exploits to target systems whose users have not yet installed the latest updates.
Source: http://www.newsfactor.com/story.xhtml?story_id=10300002P058

38. *June 19, Government Computer News* — **Department of Energy ups security efforts after loss of employee data.** The Department of Energy (DOE) has joined a long list of federal agencies that recently have suffered serious breaches of cybersecurity. Unlike those organizations, however, the DOE breach was the result of a targeted intrusion and theft, rather than carelessness. Said Alan Paller, director of research at the SANS Institute: “This is the tip of a much bigger iceberg...This is an example of the kind of attack and extraction that was going on for the last 2 1/2 years” during Titan Rain, an organized series of cyberattacks believed to have originated in China. At DOE, hackers stole personal information on 1,502 employees from an unclassified system belonging to the National Nuclear Security Administration. DOE is attacked hundreds of times a day, says Tom Pyke, DOE CIO, so he has established a departmentwide cyberincident management team. In addition, DOE has increased the use of data encryption software and has implemented twofactor authentication requirements for systems administrators at all department sites. Pyke said DOE has always reported incidents to the U.S. Computer Emergency Readiness Team. DOE is moving to strengthen its notification processes by trying "to ensure people understand it’s a good thing to report incidents,” Pyke said.
Source: http://www.gcn.com/print/25_16/41047−1.html?topic=security

39. *June 16, eWeek* — **World Cup network operators hold their breath.** Avaya officials managing the sprawling World Cup network for the Federation of International Football Associations (FIFA) are holding their breath. So far, there have been no serious attacks on the network, but if there are, they are likely to happen at the peak of the tournament. On the security side that means using automated tools −− both commercial and open source −− and humans to monitor for security events 24 hours a day. Automated tools include host intrusion detection, network intrusion detection, "a bevy of log analysis tools, anti−virus and we use

honey networks −− virtual networks that allow us to see malicious activity in real time," said Tom Porter, chief of Internet security for FIFA and Avaya in Munich, Germany. On the network side, it also means putting a lot of redundancy into the network, which spans 64 venues, 12 stadiums, two FIFA hotel headquarters in Berlin and Frankfurt, 11 other FIFA hotels, 11 organizing committees and an airport and railway station. With such precautions in place, Avaya was confident enough to guarantee 99.999 percent availability for the converged voice and data network.
Source: http://www.eweek.com/article2/0,1895,1977801,00.asp

40. *June 16, Associated Press* — **Gates to give up daily role at Microsoft.** Bill Gates isn't leaving Microsoft, he's just leaving his day−to−day responsibilities there. That was the message Microsoft Corp. sought to send Thursday, June 15, when it announced that Gates planned to step back from his regular duties in July 2008, while still continuing to be chairman of the company he co−founded. One of the key people taking on Gates' responsibilities is technology luminary Ray Ozzie, who developed Lotus Notes and came to Microsoft when it acquired his company, Groove Networks Inc., in 2005. The move will end an era at Microsoft, which Gates founded in 1975 with childhood pal Paul Allen. The Redmond company on Thursday laid out a plan for other high−ranking executives to take on Gates' duties. Gates and Chief Executive Steve Ballmer also noted that recent corporate reorganizations have been designed to move more responsibility to lower−ranking executives, so the company could more quickly make decisions without Gates and Ballmer.
Source: http://www.forbes.com/business/feeds/ap/2006/06/16/ap2819759 .html

41. *June 16, IDG News Service* — **U.S. government agencies look to efficiently convert old data.** The U.S. government's intelligence agencies are looking heavily into technology that can quickly convert typewritten and even handwritten text into electronic data, said Greg Pepus, senior director of federal outreach at In−Q−Tel, a venture capital firm funded by U.S. agencies such as the Central Intelligence Agency. Intelligence agents need technology that can quickly convert notes handwritten in Arabic or in symbols to electronic data that can be easily shared and put into a database, he said. "The problem is the vast majority of data in the world isn't in databases," Pepus said during a panel discussion about the future of U.S. government IT needs at the Gartner Inc. Government Conference 2006 in Washington, DC. In addition, In−Q−Tel is looking for better search technologies that allow wide−ranging searches across multiple databases in one interface, Pepus said.
Conference Website: http://www.gartner.com/2_events/conferences/gcon3.jsp
Source: http://www.infoworld.com/article/06/06/16/79396_HNusgovernme ntdata_1.html

Internet Alert Dashboard

DHS/US−CERT Watch Synopsis

Over the preceding 24 hours, there has been no cyber activity which constitutes an unusual and significant threat to Homeland Security, National Security, the Internet, or the Nation's critical infrastructures.

US−CERT Operations Center Synopsis: US−CERT is aware of active exploitation

of a new vulnerability in Microsoft Excel. Successful exploitation could allow an attacker to execute arbitrary code with the privileges of the user running Excel. For more information please the review the following:

Technical Cyber Security Alert: TA06−167A
http://www.us−cert.gov/cas/techalerts/TA06−167A.html

Vulnerability Note: VU#802324 http://www.kb.cert.org/vuls/id/802324

We are continuing to investigate this vulnerability. US−CERT recommends the following actions to help mitigate the security risks:

Install anti−virus software, and keep its virus signature files up to date.

Limit user privileges to no administrator rights.

Save and scan any attachments before opening them.

Review the workarounds described in Microsoft Security Advisory 921365:
http://www.microsoft.com/technet/security/advisory/921365.ms px

US−CERT strongly encourages users not to open unfamiliar or unexpected email attachments, even if sent by a known and trusted source. Users may wish to read Cyber Security Tip ST04−010 for more information on working with email attachments: http://www.us−cert.gov/cas/tips/ST04−010.html

FDIC Phishing Scam

US−CERT continues to receive reports of phishing scams that target online users. Recently, the phishing scam targeted the customers of Federal Deposit Insurance Company (FDIC) insured institutions.

Customers of FDIC institutions received a spoofed email message, which claims that their account is in violation of the Patriot Act, and that FDIC insurance has been removed from their account until their identity can be verified. The message provides a link to a malicious web site which prompts users to enter their customer account and identification information.

If you were affected by the FDIC phishing scam, please refer to the FDIC Consumer Alert for assistance: http://www.fdic.gov/consumers/consumer/alerts/phishing.html

US−CERT confirms that the federal agencies including Department of Homeland Security (DHS) mentioned in the fraudulent email have not sent out an email that requests customer account or identification information.

US−CERT encourages users to report phishing incidents based on the following guidelines:

Federal Agencies should report phishing incidents to US−CERT:
http://www.us−cert.gov/nav/report_phishing.html

Non−federal agencies and other users should report phishing incidents to OnGuard Online, a consortium of Federal Agencies: http://onguardonline.gov/phishing.html

Additionally, users are encouraged to take the following measures to prevent phishing attacks from occurring:

Do not follow unsolicited web links received in email messages.

Contact your financial institution and file a complaint with the Federal Trade Commission (FTC) immediately if you believe your account or financial information has been compromised.
https://rn.ftc.gov/pls/dod/widtpubl$.startup?Z_ORG_CODE=PU03

Review FTC's web site on how to protect yourself from identity theft:
http://www.consumer.gov/idtheft/

Review the OnGuard Online practical tips to guard against Internet fraud, secure your computer, and protect your personal information:
http://onguardonline.gov/phishing.html

Refer to the US−CERT Cyber Security Tip on Avoiding Social Engineering and Phishing Attacks: http://www.us−cert.gov/cas/tips/ST04−014.html

Refer to the CERT Coordination Center document on understanding Spoofed/Forged Email: http://www.cert.org/tech_tips/email_spoofing.html

PHISHING SCAMS

US−CERT continues to receive reports of phishing scams that target online users and Federal government web sites. US−CERT encourages users to report phishing incidents based on the following guidelines:

Federal Agencies should report phishing incidents to US−CERT.
http://www.us−cert.gov/nav/report_phishing.html

Non−federal agencies and other users should report phishing incidents to Federal Trade Commissions OnGuard Online. http://onguardonline.gov/phishing.html

Current Port Attacks

Top 10 Target Ports	1026 (win−rpc), 6881 (bittorrent), 4672 (eMule), 50497 (−−−), 38566 (−−−), 445 (microsoft−ds), 24232 (−−−), 80 (www), 25 (smtp), 32790 (−−−) Source: http://isc.incidents.org/top10.html; Internet Storm Center

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Website: www.us−cert.gov.

Information on IT information sharing and analysis can be found at the IT ISAC (Information Sharing and Analysis Center) Website: https://www.it−isac.org/.

[Return to top]

Commercial Facilities/Real Estate, Monument &Icons Sector

Nothing to report.
[Return to top]

General Sector

Nothing to report.
[Return to top]

DHS Daily Open Source Infrastructure Report Contact Information

DHS Daily Open Source Infrastructure Reports − The DHS Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary of open−source published information concerning significant critical infrastructure issues. The DHS Daily Open Source Infrastructure Report is archived for ten days on the Department of Homeland Security Website: http://www.dhs.gov/iaipdailyreport

DHS Daily Open Source Infrastructure Report Contact Information

Content and Suggestions:	Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS Daily Report Team at (703) 983−3644.
Subscription and Distribution Information:	Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS Daily Report Team at (703) 983−3644 for more information.

Contact DHS

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at nicc@dhs.gov or (202) 282−9201.

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Web page at www.us−cert.gov.

Department of Homeland Security Disclaimer

The DHS Daily Open Source Infrastructure Report is a non−commercial publication intended to educate and inform personnel engaged in infrastructure protection. Further reproduction or redistribution is subject to original copyright restrictions. DHS provides no warranty of ownership of the copyright, or accuracy with respect to the original source material.